

5 Ways Fraudsters May Lure Victims Into Scams Involving Crypto Asset Securities – Investor Alert

July 23, 2025 - Filed by: [miguelcfl](#)

The SEC's Office of Investor Education and Advocacy is issuing this Investor Alert because fraudsters continue to exploit the popularity of crypto assets to lure retail investors into scams. Crypto assets may include assets commonly referred to as cryptocurrencies, crypto, coins, and tokens.

Fraudsters often use innovations and new technologies to perpetrate investment scams, and this has been the case with crypto asset securities-related investments. While federal and state regulators continue to bring enforcement actions in this space, recovering money from the fraudsters can be difficult because it can be challenging to trace and recover funds. For example, fraudsters can use technology to obscure their identities or hide the trail of funds using crypto assets. Recovering your investment from a crypto asset-related scam can also be difficult because fraudsters can quickly send your funds overseas.

Fraudsters use a variety of techniques to convince investors to hand over their hard-earned money. Here are five things you should watch out for to avoid losing your money to a scam involving crypto assets.

Fraudsters Connect With You on Social Media Platforms or Through a Supposedly Accidental Text Message, and Then Gain Your Trust.

Fraudsters may initiate contact with potential victims on social media platforms — including professional networking, dating, and messaging websites/apps — or through unsolicited text messages. They may pretend to be an old friend or claim to have contacted you accidentally. The fraudster may quickly move communications with you away from the initial platform. The fraudster may then initiate a friendship or romantic relationship with you to build trust and convince you to invest your money before disappearing with your funds. These relationship confidence scams are sometimes referred to by a term that is as unpalatable as the fraudsters' conduct — “pig butchering scams.”

One way this type of scam can play out is that after a fraudster has established an online relationship with you, the fraudster may claim to know about lucrative investment or trading opportunities, including investments involving crypto assets. The fraudster may even indicate that a relative or friend works at a financial firm or is an “insider” and therefore is able to provide trading information. The fraudster may direct you to a legitimate-looking (but fake) website or to a widely-used app that can be downloaded from a well-known app store, make it look like you have profited, and even allow you to withdraw a small amount of “profits,” further gaining your trust. The fraudster may then ask you to invest larger sums of money. When you want to withdraw your funds, the fraudsters often come up with an excuse why that is not possible, or they may tell you for the first time that you must pay more to cover fees or taxes. Frequently, there is no way you will recover your investment or any “profits” so paying additional funds only causes you to lose more money.

For anyone you have met solely online or through an app:

Do not make investment decisions based on their advice or solicitation. Note that fraudsters may direct you to get Bitcoin at a Bitcoin ATM (or kiosk) or through a crypto platform in order to make investment deposits, and then tell you where to send that Bitcoin. Keep in mind that an investment may not be legitimate if you are required to pay for it with crypto assets.

Do not share with them any information relating to your personal finances or identity. Do not give them anything like your bank or brokerage account information, tax forms, credit card, social security number, passport, driver's license, birthdate, or utility bills.

Fraudsters Exploit the Hype Around Emerging Technologies Such as Artificial Intelligence (AI).

Fraudsters may use the growing popularity of artificial intelligence (AI) as a hook for luring investors into crypto asset securities-related investments. It might seem exciting to invest in crypto asset-related investments that have a connection to AI, but be careful. Fraudsters often use the hype around new technological developments, like emerging AI technologies, to lure investors into scams. Fraudsters may use catchy AI-related buzzwords and make claims that you will make a lot of money when their only intention is to steal your money. They may claim to deploy bots that use AI to find the best crypto asset-related investments.

Fraudsters also may use AI technology itself to produce realistic looking websites or marketing materials to promote investment scams, including crypto asset-related investment scams. Similarly, they may use AI technology to create "deepfakes" — cloning, altering or faking voices, images, and videos to deceive investors. They may even create deepfakes of celebrities, government officials, or your loved ones in order to gain your trust or to convince you to send funds.

Fraudsters Impersonate or Exploit Trusted Sources.

Be aware that communications — including phone calls, voicemails, text messages, messages via social media, emails, letters, and certificates — may falsely appear to be from official U.S. government sources, including the SEC. If you receive a communication that appears to be from the SEC, do not provide any personal information until you have verified that you are dealing with someone from the SEC, and not an impersonator.

AI technology has made it even easier for fraudsters to impersonate government agencies, organizations, and individuals in luring investors into scams. Fraudsters may even impersonate your friends or family members using AI technology to create deepfakes. They also may hack your friends' or family members' social media accounts, and then post or send messages pretending to be from them. For example, they may post that your friend or family member has become a crypto asset expert and seeks friends to join in trading or investing.

Even if you are certain that an investment pitch is coming from a friend or family member, keep in mind that they may have been fooled into believing that the investment is legitimate when it is not. Sometimes fraudsters target communities or groups by recruiting leaders or others to pitch an investment without them knowing that the "opportunity" is a scam.

Fraudsters May Pump Up the Price of a Crypto Asset and Then Sell at Your Expense.

Fraudsters may conduct pump-and-dump schemes with crypto assets, including so-called "memecoins" that refer to popular culture or internet memes. For example, fraudsters may create a memecoin and then tout it on social media — sometimes in what they refer to as a "pre-sale" — to get others to buy and "pump" up, or increase, its price. Then the promoters or others working with them "dump," or sell, before the hype ends, profiting from the pumped up price. Typically, after the promoters sell and take their profit, the price decreases rapidly, and everyone else who bought the tokens loses most of their money. Never make investment decisions based solely on information from social media platforms or apps.

Fraudsters Demand Additional Costs That They Falsely Claim Will Allow You to Withdraw From Your Account, or to Recover Losses.

In investment scams, including ones that involve crypto asset securities, fraudsters may demand that you pay additional costs, fees, or taxes to withdraw money from your account. This is an example of

an advance fee fraud, where investors are asked to pay a bogus fee upfront before receiving anything. For example, fraudsters may falsely tell you that your account has been frozen by a regulator or because a regulator is investigating your account. They may ask you to pay a large deposit, fee, or sum of taxes to unfreeze your account. If you pay, however, you are unlikely to receive your initial investment and will also lose the additional payment.

Another way fraudsters may trick you into paying additional costs is by telling you they “mistakenly” deposited money into your account and ask you to refund the money. They never actually put money in your account – it’s just a ploy to convince you to give them more money.

Fraudsters also may target you if you already have lost money or crypto assets due to bankruptcy or a scam. They may ask you to send them the private key to access your crypto assets, or to put in additional money or crypto assets, offering to “help” you recover what you lost. In reality, if you pay, you likely will not get back what you put in and will instead have been scammed again.

Don’t get caught up in the fear of missing out (FOMO) on a purported investment opportunity that seems new or “cutting-edge.” If you are considering an investment involving crypto asset securities, look out for the tactics described above and other warning signs of an investment scam.

Additional Information

Exercise Caution with Crypto Asset Securities: Investor Alert

Social Media and Investment Fraud – Investor Alert

Artificial Intelligence (AI) and Investment Fraud: Investor Alert

Digital Asset and “Crypto” Investment Scams – Investor Alert

Report possible securities fraud to the [SEC](#).